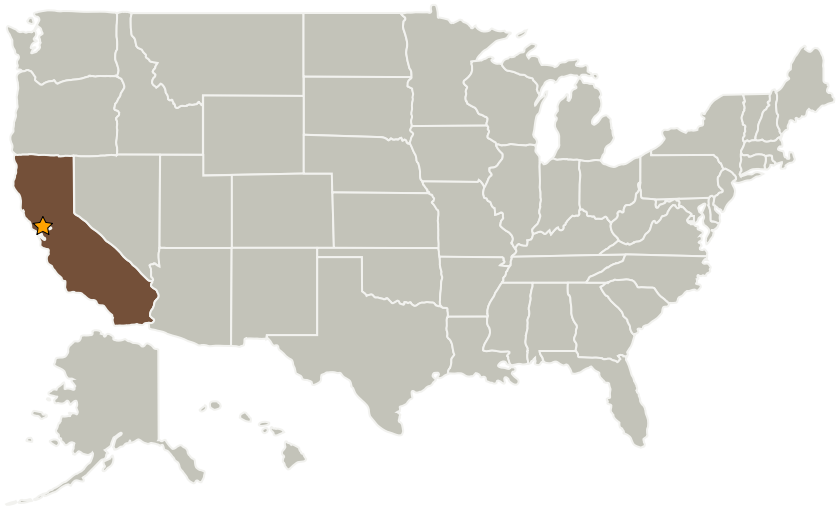
Mitigating Software Failures with Distributed and Recovery-Oriented Flight System Architectures, Phase I

Completed Technology Project (2006 - 2007)

Project Introduction

The primary focus of Integrated Vehicle Health Management (IVHM) has been on faults due to hardware failures. Yet software is growing in complexity, controls critical functionality under a wide range of conditions and does so with greater autonomy. Furthermore, software errors have negatively impacted major missions. Runtime recovery from software faults is gaining momentum in research community with major efforts such as the IBM autonomic computing effort and the Stanford/Berkeley Recovery-Oriented Computing project. We propose application of these methods to flight software in the context of JPL's Mission Data System (MDS), an integrated systems and software architecture for next-generation space missions. Specifically, we consider: ? Detection and repair of radiation induced Single Event Upsets (SEU) that can either change data values or code. ? Recovery from bugs manifested as the use of computational resources outside of a specified mode-dependent resource profile. ? Software organization and infrastructure to help diagnose and limit the impact of errors. We shall study how to restructure MDS as a distributed system with redundant hierarchical components. ? A recovery strategy based on component-level rebooting. This STTR is a cooperative project between the small business Kestrel Technology and NASA's Jet Propulsion Laboratory (JPL).

Primary U.S. Work Locations and Key Partners



Mitigating Software Failures with Distributed and Recovery-Oriented Flight System Architectures, Phase I

Table of Contents

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Center / Facility:

Ames Research Center (ARC)

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Small Business Innovation Research/Small Business Tech Transfer

Mitigating Software Failures with Distributed and Recovery-Oriented Flight System Architectures, Phase I

Completed Technology Project (2006 - 2007)

Organizations Performing Work	Role	Type	Location
★Ames Research Center(ARC)	Lead Organization	NASA Center	Moffett Field, California
Kestrel Technology LLC	Supporting Organization	Industry	Palo Alto, California

Primary U.S. Work Locations
California

Project Management

Program Director:

Jason L Kessler

Program Manager:

Carlos Torrez

Technology Areas

Primary:

- TX11 Software, Modeling, Simulation, and Information Processing
  - TX11.1 Software Development, Engineering, and Integrity
    - TX11.1.4 Operational Assurance